View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by eLibrary National Mining University

УДК 004.771

ИСПОЛЬЗОВАНИЕ RDP ДЛЯ НАПАДЕНИЯ

Стасивский Л.С.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, stasivskyj@gmail.com

Появление любой технологии сулит чаще всего и новые специфические проблемы. Конечно, терминальные службы Microsoft – понятие совсем не новое, тем не менее использовать ее в хакерских целях может быть очень даже интересно. Итак, предположим, что злоумышленник должен атаковать какую-то корпоративную сеть, а точнее, ее пользователей.

Ключевые слова – протокол удалённого рабочего стола; защита РОР-сервер.

Remote Desktop Protocol (RDP, протокол удалённого рабочего стола) позволяет пользователям удаленно работать на хосте, используя нативный графический интерфейс. Но как можно атаковать пользователей, обладая доступом к РОР-серверу? Самый простой вариант лежит в возможности автоматического монтирования дисков и устройств клиента при подключении к РОР-серверу. То есть при подключении пользователя к РОР-серверу диски становятся доступными для РОР- сервера и у него появляется возможность поместить на клиент любые файлы в любое место (в зависимости от прав пользователя в своей ОС). Конечно, по умолчанию диски не монтируются, но здесь есть некоторые тонкости.

Во-первых, через стандартный РОР-клиент (mstsc) нет возможности задавать, при подключении к какому серверу монтировать диск, а к какому – нет. Там используются общие настройки для всех подключений. Таким образом, достаточно часто получается, что администраторы “ходят” на РОР по серверам с подключенными дисками, и это создает прекрасную основу для атаки. По сути, нужно захватить контроль над одним из серверов и тем или иным образом заставить администратора зайти на него, а далее все информация становится доступной.

Во-вторых, можно принудительно включить опцию подключения дисков – за счет указания соответствующих настроек в РОР- файлах. И это дает несколько иной вектор атаки – атаку на офисных пользователей. Суть заключается в том, что злоумышленник может создать такой РОР-файл, при запуске которого у пользователя ничего спрашиваться не будет, а автоматически произойдет подключение к RDP-серверу с автомонтированием дисков и последующим захватом контроля пользовательским компьютером. Конечно, здесь потребуется проявить немного социальной инженерии. Например, можно разослать офисным работникам письма с приложенными РОР-шками и просьбой их запустить для тестирования какой-то новой системы. Такие файлы не вызовут подозрения у офисных работников, и, большинство выполнит необходимые действия.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Обновление возможностей Remote Desktop Services в Windows Server 2012.(Электрон. ресурс) / Способ доступа: URL: http://habrahabr.ru/company/microsoft/blog/167289 - Обновление возможностей Remote Desktop Services в Windows Server 2012.
2. Remote Desktop Protocol (RDP). (Электрон. ресурс) / Способ доступа: URL: http://en.wikipedia.org/wiki/Remote_ Desktop_Protocol – Remote Desktop Protocol (RDP).